Numbers and Sets Notes

Based on Lectures and "The Higher Arithmetic"

$\theta\omega\theta$

Not in University of Cambridge
skipped some talks irrelevant to contents

E-mail: not telling you

Contents

Elementary Number Theory

Pre: Introduction

- Number theory $\Rightarrow$ The reals $\Rightarrow$ Sets and functions $\Rightarrow$ Countability
- Recommended books: Allenby: âĂIJNumbers and ProofsâĂİ; Hamilton: âĂIJNumbers, sets and functionsâĂİ; Davenport: âĂIJThe Higher ArithmeticâĂİ

1 Preliminaries

1.1 Q and A

- Q: What is a proof? A: A proof is a *logical argument* that establishes a *conclusion*.
- Q: Why do we prove things? A:
  - To be sure they are true.
  - To understand why they are true.

1.2 Examples of Proofs and non-Proofs

I $\forall n \in \mathbb{N}^*, 3|n^3 - n$.

II $\forall n$, if n^2 is even then n is even.

III For any $n \in \mathbb{N}*$, if $9|n^2$ then $9|n$.

This is a *wrong* claim. A counterexample is $n = 3$.

Definition of if and only if, ..., skipped

2 The Natural Numbers

Definition 2.1. The set of natural numbers $\mathbb{N}$ is a set containing an element âĂIJ1âĂİ and with an operation âĂIJ+1âĂİ satisfying

(1) $\forall n \in \mathbb{N}, n + 1 \neq 1$.

(2) If $m \neq n$, then $m + 1 \neq n + 1$.

(3) (Induction Axiom) For any property $P(n)$, $(P(1) \wedge P(n) \Rightarrow P(n+1)) \Rightarrow \forall n \in \mathbb{N}(P(n))$.

They are called the *Peano axioms*.

These two rules ensure that all natural numbers are different.

Thus we can define $+k$ recursively by $2 = 1 + 1$, and $n + (k + 1) = (n + k) + 1$. Other usual operations can be defined similarly. Usual laws of arithmetic can be derived by induction.

Proposition 2.1 (Strong induction). $(P(1) \wedge \forall n(\forall m \leqslant n, P(m) \Rightarrow P(n+1))) \Rightarrow \forall n(P(n))$.

Remark. Some equivalent forms of strong induction:

1. If $P(n)$ fails for some n, then we have a minimum element n' such that $P(n')$ is false but $P(m)$ is true for all $m \leqslant n'$.
2. If $P(n)$ for some n then there is a least n with $P(n)$.

   Often referred as the *well-ordering principle*.

3 The Integers

Written in $\mathbb{Z}$, consist of all symbols $n, -n, n \in \mathbb{N}$ and 0. Usual laws hold.

Expand definition of order by $a < b$ if and only if $\exists c \in \mathbb{N}$, $a + c = b$. We have

$$\forall a, b, c, a < b \wedge c > 0 \implies ac < bc.$$

4 The Rationals

Written in $\mathbb{Q}$, consists of all expressions $a/b, a, b \in \mathbb{Z}, b \neq 0$ with a/b regarded as c/d if $ad = bc$.

Addition is defined as

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}.$$

This holds however we write those fractions.

Remark. Unlike clear unambiguity in $\mathbb{Z}$, we cannot define operations like $a/b \mapsto a^2/b^3$.

All usual laws work, with order defined as $a/b < c/d (b, d > 0)$ if and only if $ad < bc$.

5 Primes

Definition 5.1. m is said to be a *divisor* of n if and only if $\exists k \in \mathbb{N}, n = km$.
$p \in \mathbb{N}$ is *prime* if and only if only 1 and p divide p.

Proposition 5.1. Every natural numebr $n \geqslant 2$ is expressible as a product of primes.

Proved by induction. Lecture 4.

Theorem 5.1. There are infinitely many primes.

Definition 5.2. For $a, b \in \mathbb{N}$, a natural number c is the hcf of a, b if $c|a \wedge c|b$ and $d|a \wedge d|b \Rightarrow d|c$.

Proposition 5.2. Let n, k be natural numbers. Then $\exists q, rin\mathbb{Z}, 0 \leqslant r < k$ that $n = qk + r$.

Theorem 5.2 (Euclid's Algorithm)**.** skipped